ESTADO DE CHIAPAS

INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADOS DE CHIAPAS

DOCUMENTO DE SEGURIDAD

PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES

TUXTLA GUTIÉRREZ, CHIAPAS; ENERO DE 2023

itaipch
INSTITUTO DE TRANSPARENCIA
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES
CHIAPAS TRANSPARENTE

CONTENIDO

PRESENTACIÓN

Con fundamento en el artículo 19 de la Declaración Universal de Derechos Humanos, el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, artículo 13 del Pacto de San José, el artículo IV de la Declaración Americana de los Derechos y Deberes del Hombre, artículo 4 de la Carta Democrática Interamericana en tanto que en el orden Jurídico Nacional tiene su base en el artículo 6 apartado A, fracciones I y II de la Constitución Política de los Estados Unidos Mexicanos, en los que incorpora que toda persona tiene derecho al libre acceso a la información plural y oportuna yal derecho a la protección de sus datos personales, así como al acceso, rectificación, cancelación, oposición y portabilidad en los términos que determina la Ley.

En este sentido la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del estado de Chiapas, establece un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentra en posesión de sujetos obligados, entre los que figura el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas.

En observancia de esta ley y de conformidad con el artículo 45, se ha diseñado el presente documento de seguridad que tiene como propósito establecer los parámetros que guían el tratamiento de los datos personales al interior del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, por las diferentes unidadesadministrativas que lo conforman.

En ese sentido, el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, ha identificado los procesos que en el ámbito de su competencia involucran el tratamiento de datos personales, a efecto de mantener la seguridad de los mismos durante el ciclo de vida de la información, indicando la forma en la que se trata, las medidas de seguridad adoptadas y las áreas responsables de su protección, así como las finalidades del tratamiento de acuerdo a sus respectivos ámbitos de funciones.

El Documento de Seguridad busca crear un sistema de gestión para el tratamiento de los datos personales, que integre las acciones interrelacionadas para operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales.

Esto implica el planteamiento de acciones pertinentes para evitar la alteración, pérdida, transmisión y acceso no autorizado de los datos mediante la implementación de medidas físicas, administrativas y técnicas, tendientes a garantizar la seguridad e integridad de dichos datos con el seguimiento y observancia continua. Incluye además acciones que permitan controlar y verificar que el tratamiento de los datos personales se realice de acuerdo con los principios establecidos para la protección de los datos personales, implicando un compromiso con las disposiciones previstas en la ley y en los lineamientos generales, por parte de los funcionarios involucrados.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, es necesario señalar que todos y cada uno de los elementos que lo integran, constituyen un sistema interno para la gestión y tratamiento de los datos personales en posesión del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, tal como lo indica el artículo 34 de la Ley de Protección de Datos Personales en posesión de sujetos obligados del estado de Chiapas, se entiende por sistema de gestión, al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

Finalmente, ante la necesidad de mantener actualizado el documento de seguridad se ha de procurar su mejora continua. Además, se ha procedido a la actualización de los elementos que integran el documento de seguridad; las medidas de seguridad adoptadas en su tratamiento, el análisis de riesgo y brecha, que permiten dar seguimiento a las medidas adoptadas, identificar las posibles vulneraciones y aminorar los riesgos. Todo lo anterior, acompañado del desarrollo del programa de capacitación que permita comprender la importancia de adoptar medidas para la prevención de las vulneraciones a los datos personales.

1. OBJETIVOS DEL DOCUMENTO DE SEGURIDAD

El presente documento tiene como objetivo:

Ofrecer el marco de trabajo necesario para la protección de los datos personales en posesión del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, como un medio para cumplir con las obligaciones que establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas (LPDPPSOCHIS) y los Lineamientos Generales, así como la normatividad que derive de los mismos; estableciendo los elementos y actividades de gestión para la operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, además de promover la adopción de mejores prácticas en relación con la protección de datos personales, con la finalidad de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, emite el presente documento

.

2. RESPONSABILIDADES

De conformidad con lo dispuesto por el artículo 113 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas (LPDPPSOCHIS), el Comitéde Transparencia es la autoridad máxima en materia de protección de datos personales, teniendo entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, en esa tesitura dicho órgano tiene las siguientes funciones con relación a este programa:

I. Elaborar, aprobar, coordinar y supervisar el Programa, en conjunto con las áreas técnicas que estime necesario involucrar o consultar;
II. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
III. Dar a conocer el Programa al interior del sujeto obligado;
IV. Coordinar la implementación del Programa en las unidades administrativas del sujeto obligado;
V. Asesorar a las unidades administrativas en la implementación de

este Programa, con el apoyo de la Dirección de Capacitación;

VI. Presentar un informe anual al titular de la institución, en el que se describan las acciones realizadas para cumplir con lo dispuesto por este Programa;

VII. Supervisar la correcta implementación del Programa;

VIII. Elaborar, aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con las áreas técnicas que estime necesario involucrar o consultar, y

IX. Las demás que de manera expresa señale el propio Programa.

Las unidades administrativas, el área coordinadora de archivos y la unidad de transparencia tendrán las funciones y responsabilidades que se describen más adelante en este documento.

Para que los objetivos planteados se logren con éxito, el Programa requiere del apoyo e impulso directo del más alto nivel de la institución. En ese sentido, el Programa **se deberá hacer del conocimiento** del Pleno y la Presidencia del Instituto, a fin de que tomen las medidas necesarias para que el mismo se observe en este Instituto.

La intervención del Comisionado Presidente tendrá la finalidad de impulsar la debida implementación del Programa al interior del sujeto obligado, pero no podrá suplir ni afectar las funciones del Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la organización.

Asimismo, para que la implementación del Programa tenga como resultado el cumplimiento integral de las obligaciones que establece la LPDPPSOCHIS y los Lineamientos Generales, el Programa **será de observancia obligatoria para todas las personas servidoras públicas del sujeto obligado** que en el ejercicio de sus funciones traten datos personales.

Las unidades administrativas deberán realizar las acciones necesarias para cumplir con las obligaciones que establece este Programa, para lo cual deberán asignar los recursos materiales y humanos necesarios, y prever lo que se requiera en sus programas de trabajo.

Para ello, resulta fundamental que el Programa se conozca al interior del sujeto obligado, por lo que el Comité de Transparencia se encargará de difundirlo y socializarlo entre el personal.

3. ALCANCE DEL DOCUMENTO DE SEGURIDAD

El documento de seguridad aplica a todas las unidades administrativas que realicen tratamientos de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que efectúen, mismos que se encuentran bajo su estricta responsabilidad, tanto en los espacios físicos como los medios electrónicos en los que se resguardan, operan y administran, con observancia de los principios, deberes y obligaciones que establece la ley.

Las unidades administrativas que forman parte del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas y que deberán observar el Programa de Protección de Datos Personales son las siguientes:

- Dirección de Administración y Finanzas
- Dirección Jurídica
- Dirección de Verificación y Tecnologías de la Información
- Dirección de Capacitación y Promoción de la Transparencia
- Dirección de Comunicación y Vinculación Social
- Unidad de Transparencia
- Área Coordinadora de Archivos

La Dirección de Capacitación y Promoción de la Transparencia integra este Documento de Seguridad con base en la información generada por las citadas unidades administrativas.

4. SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES

El Sistema de Gestión de Datos Personales es el medio por el cual el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas garantiza el tratamiento de los datos personales que lleva a cabo como parte de sus funciones, desde su obtención, uso, registro, conservación,

acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación correspondiente; para lo cual, se establecen políticas y métodos orientados a salvaguardar la confidencialidad, integridad y disponibilidad de estos datos, de acuerdo con Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del estado de Chiapas y la Ley General de Transparencia y Acceso a la Información Pública del estado de Chiapas.

Por lo anterior, se inició un proceso de organización y planeación de los medios para la protección de datos, tomando como punto de partida la identificación de los procesos y tareas en los que, conforme a sus atribuciones, las distintas áreas del instituto desarrollan tratamientos de datos personales. Para tal fin, se elaboró un formulario que facilitó a cada unidad administrativa, la identificación de los tratamientos que llevan a cabo como parte de su responsabilidad, considerando lo establecido en el artículo 47 de la Ley de Protección de Datos Personales del Estado de Chiapas; logrando con ello el levantamiento del inventario de datos, tratando de identificar, lacategoría y tipo datos usados en cada tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las basesfísicas o electrónicas de datos; las finalidades del tratamiento, el nombre, cargo y adscripción de los servidores públicos que tienen acceso al tratamiento, además desi son objeto de la transferencia y la identificación de los destinatarios o receptoresde los mismos, así como las causas que la justifican.

Además, el inventario ha contribuido para la determinación del ciclo de vida de los datos personales, entendiendo que, una vez concluida la finalidad de los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, vinculado con el proceso de gestión documental que se desarrolla al interior del Instituto de Transparencia.

Una vez integrados los inventarios de tratamientos y de datos, se estableció la metodología para el análisis de riesgo, con la intención de que se identificaran el valor de los datos y su ciclo de vida, así como el valor de exposición, las posibles consecuencias para los titulares por el uso indebido y/o posible vulneración y las condiciones de riesgo a los que podrían encontrarse expuestos por medidas de seguridad poco confiables. Lo anterior, permitió identificar la brecha entre las

medidas de seguridad existentes y las medidas de seguridad faltantes para que garanticen la seguridad de los datos, tanto administrativas, como físicas y técnicas.

A partir de esta identificación de posibles vulneraciones es factible prevenir posibles debilidades en la seguridad de los datos y las áreas de oportunidad, aun cuando no haya existido un daño real, mediante la identificación de la ineficiencia de los controles de acceso físico, electrónico y el inadecuado establecimiento de los esquemas de privilegios, sumado al poco conocimiento de procesos y responsabilidades en materia de protección de datos personales, además de la falta de definición de perfiles y roles, falta de seguimiento y monitoreo a las medidas de seguridad, así como la inexistencia de mecanismos para garantizar la confidencialidad por parte del personal.

Las amenazas que se buscan prevenir pueden ser de diferentes tipos:

- Robo, extravío o copia no autorizada
- Uso, acceso o tratamiento no autorizado
- Daño, alteración o modificación no autorizado
- Pérdida o destrucción no autorizada

El riesgo que puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada comprometiendo su confidencialidad, disponibilidad e integridad; y en este sentido, las medidas de seguridad por parte de cada dirección están orientadas justamente a proteger los datos personales. En el marco del sistema de gestión y política de seguridad institucional, se procurará:

- Tratar a los datos personales conforme a la Ley;
- Identificar a los servidores públicos de este Instituto responsables del tratamiento de los datos personales.
- Que los tratamientos de datos personales estén sujetos al principio de consentimiento siempre que la Ley lo permita;
- Responder al principio de información a los titulares sobre el uso que dará y sus finalidades;
- Mantener la actualización y pertinencia de los datos personales;
- Priorizar la supresión de los datos personales cuando haya concluido el proceso para el que fueron obtenidos;

- Ajustar el tratamiento de los datos personales a las finalidades para la que fueron obtenidos y estrictamente los necesarios para las finalidades;
- Obtener datos personales a través de medios legales, con respeto a la expectativa de privacidad del titular;
- Velar por el cumplimiento de los principios, estableciendo y manteniendo medidas de seguridad y de confidencialidad durante el ciclo de vida de los datos personales, en estricto respeto de los derechos de los titulares;
- Mantener actualizado el inventario de datos personales que maneja el Instituto;

Buscando el logro de lo anterior, y tomando como punto de partida la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que, de acuerdo con otras experiencias y mejores prácticas tomadas como referencia, se encaminan a la mejora continua por parte de las personas involucradas en el tratamiento, en la búsqueda de lograr la salvaguarda del derecho a la privacidad y protección de datos personales, se han determinado las líneas de acción para el personal encargado de tratamiento de datos, con el propósito de generar mecanismos para el resguardo adecuado, actuando en apego a la LPDPPSO de Chiapas y los lineamientos correspondientes.

5. INVENTARIO DE TRATAMIENTOS Y DATOS PERSONALES

Para el debido cumplimiento de las obligaciones es necesario que cada una de las unidades administrativas realicen un diagnóstico de los tratamientos de datos personales que llevan a cabo.

El diagnóstico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en este Instituto.

Por “inventario de tratamientos de datos personales” se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas del Instituto, realizado con orden y precisión.

Así, en coordinación con las áreas, como resultado del proceso de análisis y actualización de la información, se logró identificar a las unidades administrativas

que realizan tratamientos con datos personales, las cuales son:

- Dirección de Administración y Finanzas
- Dirección Jurídica
- Dirección de Verificación y Tecnologías de la Información
- Dirección de Capacitación y Promoción de la Transparencia
- Dirección de Comunicación y Vinculación Social
- Unidad de transparencia
- Área Coordinadora de Archivos

Estos tratamientos se realizan en absoluto apego a sus funciones, a través de las diversas áreas que las integran y permiten el desarrollo de los procesos que realizan, para el cumplimiento de dichas funciones. En relación con lo anterior, fue posible identificar 26 procesos que se desarrollan, que implican el tratamiento de datos personales. Mismas que a continuación se describen:

UNIDAD ADMINISTRATIVA	PROCESO O TRATAMIENTO
DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS	Afiliaciones de Seguro Social
	Consentimiento de Seguro de Vida
	Credencialización
	Expediente de prestadores de servicio social y prácticas profesionales
	Expediente único de personal
	Nómina de pago de personal
	Registro de asistencia del personal
	Procedimiento de contratación y pago a proveedores
DIRECCION JURIDICA	Atención a personas sobre medios de impugnación
	Convenios de colaboración, concertación y/o prestación de servicios.
	Denuncias por incumplimiento a las obligaciones de transparencia
	Juicios y/o procedimientos seguidos en forma de juicio
	Recursos de revisión en materia de acceso a la información pública
	Recursos de revisión en materia de protección de datos personales
	Registro de unidades de transparencia e integrantes del Comité de Transparencia en el directorio de sujetos obligados
	Integración de expedientes relacionadas a las verificaciones a sujetos obligados.

DIRECCIÓN DE VERIFICACIÓN Y TECNOLOGÍAS DE LA INFORMACIÓN	Integración de expedientes de dictámenes de verificación con relación a las denuncias por incumplimiento a las obligaciones de transparencia.
	Altas, bajas y modificaciones de catálogos de los sujetos obligados en la PNT.
	Asesoría y capacitación a sujetos obligados en el proceso interno de la PNT.
DIRECCIÓN DE CAPACITACIÓN Y PROMOCIÓN DE LA TRANSPARENCIA	Inscripción y registro de asistencia a cursos de capacitación
	Programa de Protección de Datos Personales
DIRECCIÓN DE COMUNICACIÓN Y VINCULACIÓN SOCIAL	Difusión y comunicación de información
	Registro para Eventos
UNIDAD DE TRANSPARENCIA	Solicitudes de acceso, rectificación, cancelación y oposición de datos personales
	Solicitudes de acceso a la información pública
ÁREA COORDINADORA DE ARCHIVOS	Administración y resguardo de los documentos de archivos, originados por las funciones de este Instituto

Como resultado del proceso de análisis, se identificaron también los datos personales utilizados en los tratamientos, mismos que corresponden a las tres categorías, tal como se señala a continuación:

De identificación

- Nombre, firma, domicilio, CURP, RFC, número de seguridad social, cédula profesional, año de nacimiento o edad, antecedentes laborales, características físicas, correo electrónico, Curriculum vitae, datos académicos, datos de identificación, datos laborales, datos familiares, datos personales contenido en documento para acreditar personalidad del representante, datos personales contenidos en la identificación oficial presentada por la persona física, datos sindicales, descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil, entre otros),imagen en fotografía y/o video, huella dactilar, huella digital, menor de edad, clave de elector, estado civil, teléfono, sexo, nacionalidad, nivel educativo, ocupación, sexo, títulos profesionales.

Patrimoniales

- Número de cuentas bancarias, estados de cuenta, CLABE interbancaria, institución bancaria, facturas, beneficiarios, datos contenidos en declaraciones patrimoniales, descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil, entre otros).

Sensibles

- Circunstancias socioeconómicas, creencias religiosas, filosóficas o morales, datos de salud, datos sobre procedimientos judiciales o seguidos en forma de juicio, discapacidad, estado de interdicción o incapacidad legal. información genética, información migratoria, lengua indígena, origen étnico o racial, otros datos biométricos, pertenencia a pueblo indígena.

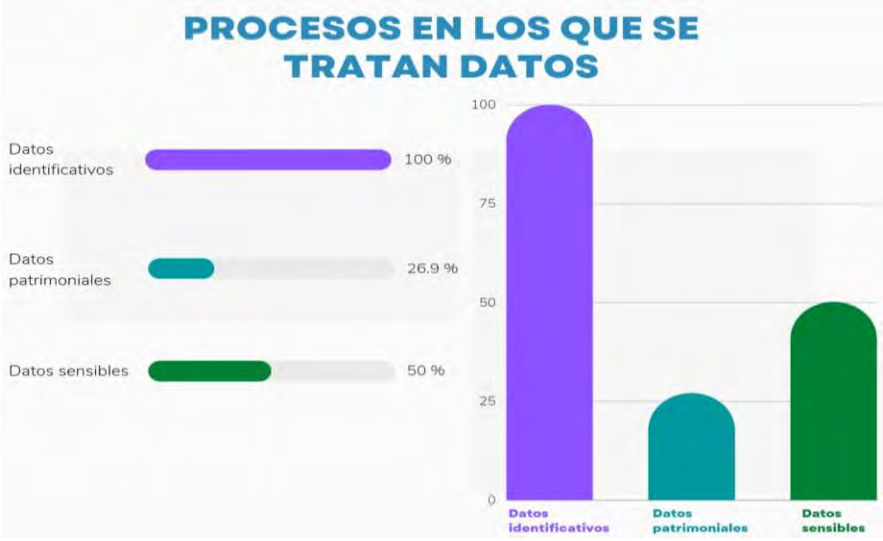
Estos datos son utilizados en 26 procesos, de los cuales ocho le corresponden a la Dirección de Administración y Finanzas, siete a la Dirección Jurídica, cuatro a la Dirección de Verificación y Tecnologías de la Información mientras que, a las Direcciones de Capacitación y Promoción de la Transparencia, Comunicación y Vinculación Social, y la Unidad de Transparencia realizan dos tratamientos cada una, y en lo que respecta al Área Coordinadora de Archivos solo tiene un proceso. Asimismo, en 26 procesos se utilizan datos personales de identificación, mientras que en 7 se recabaron datos personales patrimoniales y en lo que se refiere a datos sensibles, se manejan en 13 tratamientos.

Como se puede apreciar, la unidad administrativa con mayor número de procesos es la Dirección de Administración y Finanzas con 8 procesos, mientras que la Área Coordinadora de Archivos es la que menos procesos desarrolla, al tener solo un tratamiento.

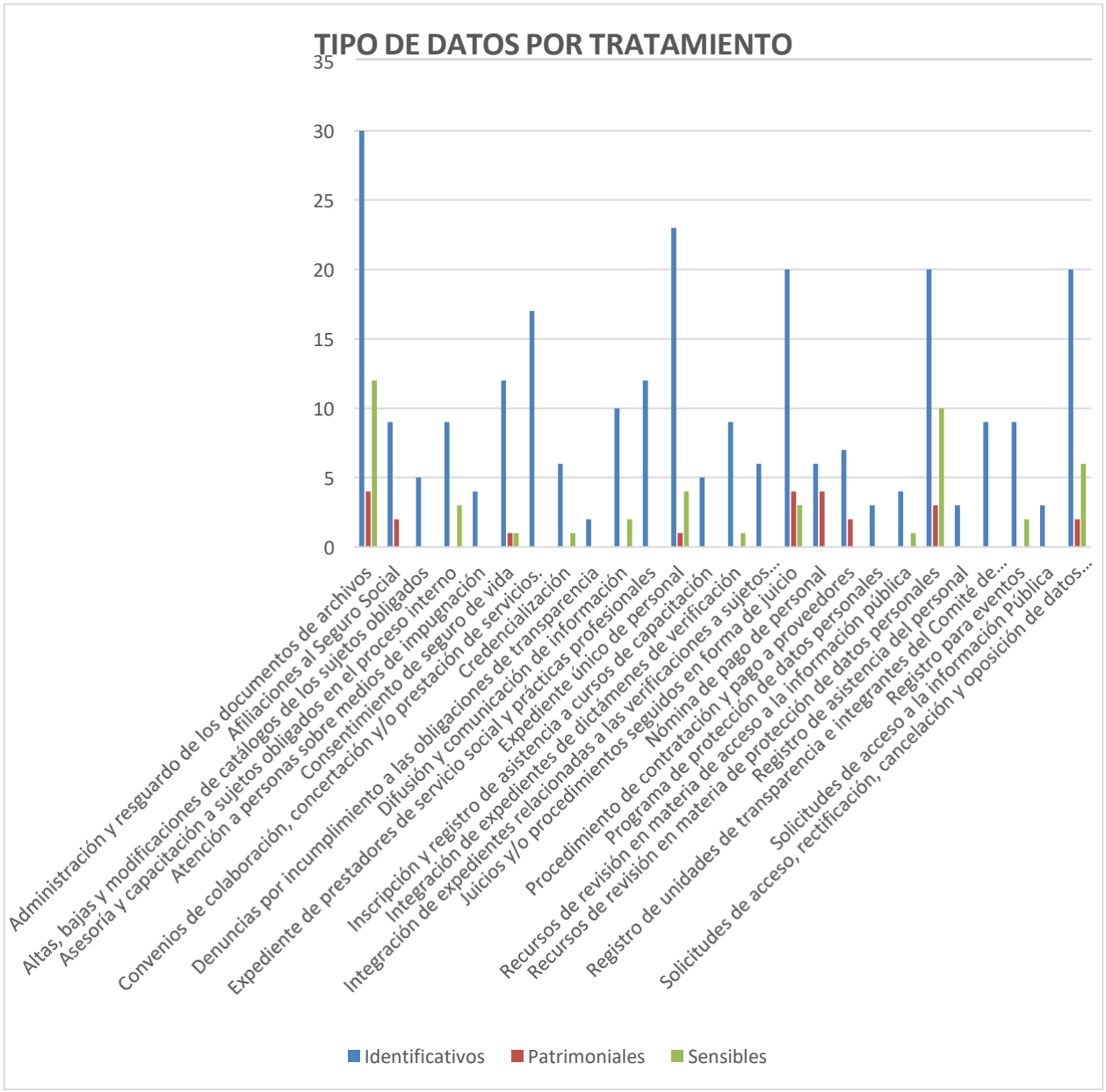
En relación con los datos solicitados, todas las unidades administrativas solicitan datos de identificación, mientras que la Dirección de Administración y Finanzas, la Dirección Jurídica, la Unidad de Transparencia y el Área Coordinadora de Archivos solicitan datos patrimoniales, por otro lado, todas las unidades administrativas con

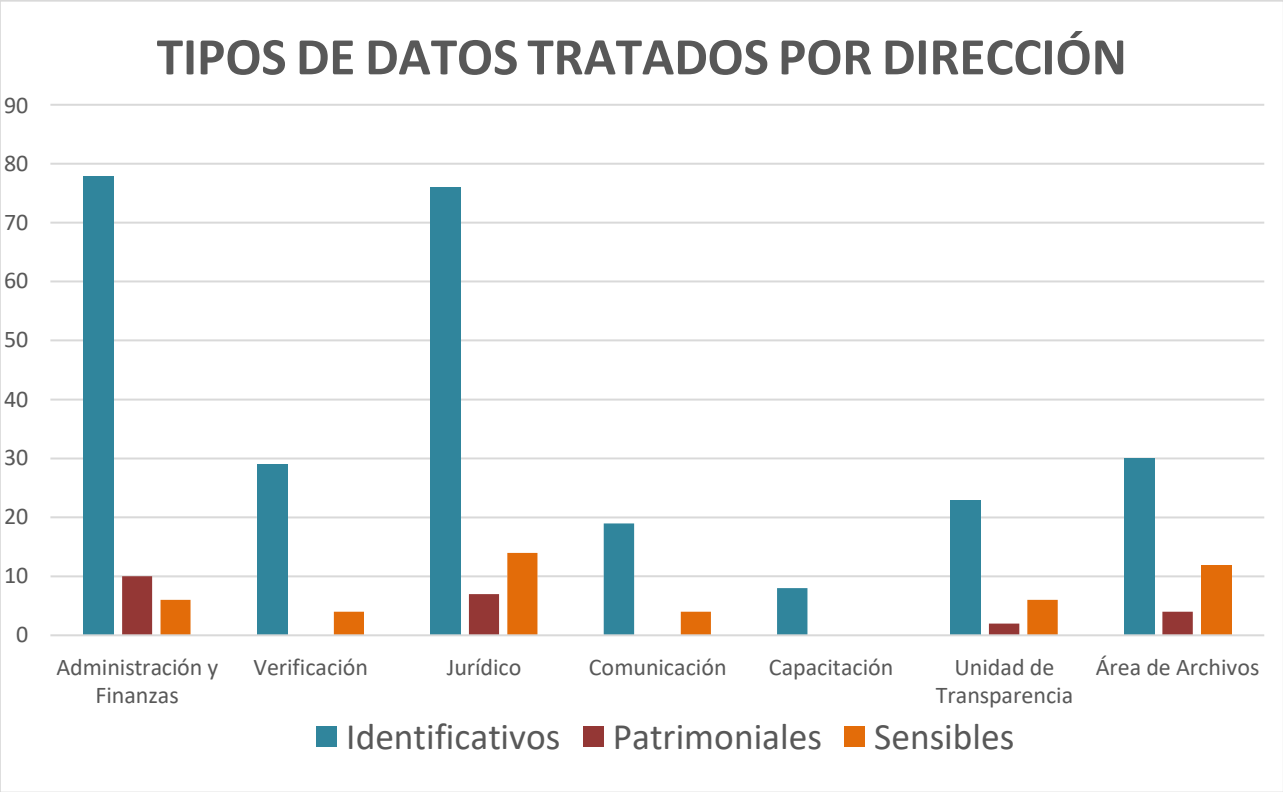
excepción de la Dirección de Capacitación manejan datos sensibles; tal como se presenta en la gráfica.

En este sentido, se identificó también que, con relación a los procesos en los que se tratan datos, el 100 por ciento de los tratamientos usan datos identificativos, el 26.9 porciento usa datos patrimoniales, y el 50% usa datos sensibles, como se muestra a continuación:



A partir de lo anterior, podemos identificar que la categoría de datos personales con mayor número procesos es la de carácter identificativo, en segundo término, los que incluyen datos sensibles y, en el caso de datos patrimoniales, contamos con seis tratamientos en los que se utilizan.





Es posible apreciar que la Dirección de Administración y Finanzas es la unidad administrativa que desarrolla el mayor número de procesos en los que intervienen tratamientos de datos personales, dada la naturaleza de sus funciones, lo anterior, debido a que las áreas que la integran cuentan con atribuciones para administrar los recursos humanos, materiales y financieros del Instituto; lo cual implica que los procesos correspondientes a la protección de datos personales sean aplicados con mayor cuidado y puntualidad, a manera de garantizar que este derecho se cumpla. No obstante, en las otras áreas, aunque en menor medida, se implementa algún tipo de proceso con tratamiento de datos; por tanto, la estrategia de protección debe ser entendida como una acción de frecuencia generalizada.

Al respecto, se identificó que cada unidad administrativa tiene un medio propio para obtener los datos personales, y estos son: físicamente, correo electrónico, Internet o sistema informático, vía telefónica, Plataforma Nacional de Transparencia, y

servicios de mensajería instantánea (WhatsApp); siempre directamente del titular. Cada unidad también se encarga de desarrollar estrategias para la protección de los datos personales, mediante archivos o bases de datos electrónicas simples, resguardadas en las computadoras de las personas servidoras públicas. No existe un sistema de base de datos institucional en el que puedan albergarse los datos personales.

Es por ello, que el Inventario de Datos del Instituto, a partir de los hallazgos identificados en su actualización, se integra como un elemento del Sistema de Gestión de Datos Personales, que representa, junto con las medidas de seguridad, un instrumento útil para la implementación de las medidas correspondientes en materia de protección de datos personales.

En este mismo sentido, ayuda a trazar las rutas para la capacitación en materia de protección de datos hacia los funcionarios del Instituto, como una vía de fortalecimiento en la operación de los procesos en que se tratan datos, en la búsqueda de sensibilizar y preparar a los responsables y encargados de los mismos, para que el tratamiento se realice de conformidad con los estándares nacionales e internacionales en la materia. En apego a lo anterior, el Inventario de Datos Personales del Instituto de Transparencia, se consolida como un elemento más de la política implementada para la observancia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en su artículo 35 párrafo I, dando certeza a la ciudadanía sobre el destino de los datos recabados por este Órgano Garante.

6. FUNCIONES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES

Como resultado de la identificación de los procesos en los que intervienen datos personales, relacionado en el Inventario de Datos Personales, por las áreas que integran las unidades administrativas correspondientes al interior del Instituto, resulta importante definir estas actividades con las funciones y facultades establecidas en el Reglamento Interior, que otorga a las personas servidoras públicas responsables de dicho tratamiento; lo anterior, a fin de dar cumplimiento al principio de legalidad que debe atender todo servidor público. Por lo anterior, a continuación,se ilustran las funciones otorgadas por el reglamento interior de este Instituto a quienes llevan a cabo tratamientos de datos personales.

UNIDAD AMINISTRATIVA	NOMBRE Y CARGO DE LA(S) PERSONA(S) FUNCIONARIA(S) QUE TRATA(N) DATOS PERSONALES	TRATAMIENTOS
Dirección de Administración y Finanzas	**C.P. Imelda Guadalupe Gutiérrez Galdámez/** Responsable de Área Recursos Humanos	Afiliaciones de Seguro Social
		Consentimiento de Seguro de Vida
		Credencialización
		Expediente único de personal
		Expediente único de personal
		Nómina de pago de personal
		Registro de asistencia del personal
	C.P. Nuria Anhel Díaz Morales Responsable de Área de Recursos Financieros, Presupuesto y Contabilidad **C.P. Elín García Ríos** Responsable de Área de Recursos Materiales y Servicios Generales	Procedimiento de contratación y pago a proveedores
Dirección Jurídica	**Mtro. Aben Amar Rabanales Guzmán** Director Jurídico **Lic. Humberto Javier Ozuna Nulutagua** Proyectista **Lic. Julio César Santoyo Lozano** Proyectista **Lic. Cynthia del Carmen Martínez Montero** Proyectista **Lic. Florinda Enedina Galindo Bonilla** Proyectista **Lic. Ángel Luis Matías Ruiz** Proyectista	Atención a personas sobre medios de impugnación
		Convenios de colaboración, concertación y/o prestación de servicios.
		Denuncias por incumplimiento a las obligaciones de transparencia
		Juicios y/o procedimientos seguidos en forma de juicio
		Recursos de revisión en materia de acceso a la información pública
		Recursos de revisión en materia de protección de datos personales
		Registro de unidades de transparencia e integrantes del Comité de Transparencia en el directorio de sujetos obligados.
Dirección de Verificación y Tecnologías de la Comunicación	**Dr. Arturo Noitier Herrera Molina** Director **Ing. Jorge Javier Coello Coutiño** Responsable de Tecnologías **Lic. Sandra Isabel García Muñoz** Verificador **Lic. David Alfonzo Cancino** Verificador	Altas, bajas y modificaciones de catálogos de los sujetos obligados en la PNT.
		Asesoría y capacitación a sujetos obligados en el proceso interno de la PNT.
		Integración de expedientes de dictámenes de verificación con relación a las denuncias por incumplimiento a las obligaciones de transparencia.

	Lic. Juan José Hernández López Verificador	Integración de expedientes relacionadas a las verificaciones a sujetos obligados.
Dirección de Capacitación y Promoción de la Transparencia	**Dra. Rosario Gpe. Chávez Moguel** Directora **Lic. Nancy Fernanda Witrón Álvarez** Auxiliar de Procesos **Lic. Norma Elizabeth Gómez Ruiz** Responsable de Área de Datos Personales y Gobierno Abierto	Inscripción y registro de asistencia a cursos de capacitación Programa de Protección de Datos Personales
Dirección de Comunicación y Vinculación Social	**Lic. José Luis Estrada Gordillo** Director **Lic. Giovanni Idali León Muñoz** Auxiliar de diseño e imagen institucional	Difusión y comunicación de información Registro para Eventos
Unidad de Transparencia	**Dra. Delia Estrada Sánchez** Responsable	Solicitudes de acceso a la información Pública Solicitudes de acceso, rectificación, cancelación y oposición de datos personales
Área Coordinadora de Archivos	**Mtra. Leydy Esthela Colmenares Jiménez** Responsable	Administración y resguardo de los documentos de archivos, originados por las funciones de este Instituto

7. ANÁLISIS DE RIESGO

De acuerdo con el artículo 50 de la LPDPPSOCHIS, el análisis de riesgo y brecha forma parte del documento de seguridad, como un medio para identificar las medidas de seguridad implementadas y, en relación con ello, las amenazas de vulneración en que se encuentran los datos personales.

El análisis sirve para identificar el riesgo inherente a los datos personales en el tratamiento a que son sometidos en el ejercicio de las funciones del Instituto, con respeto a la integridad de las personas.

La evaluación de riesgos de los datos personales forma parte de la serie de elementos que integran el documento de seguridad, cuyo propósito es garantizar la confidencialidad, integridad y disponibilidad de los datos personales en posesión del Instituto.

Asimismo, para el análisis de riesgo se han tomado en cuenta lo establecido en los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas, que en su artículo 55, define que para el cumplimiento al artículo 47 fracción IV de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del estado de Chiapas, el responsable deberá realizar un análisis de riesgo de los datos personales tratados considerando lo siguiente:

a. Los requerimientos regulatorios, código de conducta o mejores prácticas de un sector específico;
b. El valor de los datos personales de acuerdo con su clasificación previamente definitiva y su ciclo de vida;
c. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
d. Las consecuencias y negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; y
e. Los factores previstos en el artículo 47 de la Ley Estatal.

Bajo esta premisa, para analizar los riegos de los datos personales que son objeto de tratamiento por el Instituto, se aplicó un instrumento para clasificar los datos utilizados, a partir de la categorización existente en la ley:

i. **Datos de identificación o contacto**:

Que se refieren a información por la que se identifica a una persona y/o permiten su contacto como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población, edad, entre otros.

ii. Datos Patrimoniales

Son aquellos que comprenden la información que se encuentra vinculados al patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.

iii. Datos Sensibles

Se refiere a la información concerniente a la esfera más íntima de su titular

o que su uso puede dar origen a discriminación o conlleve a un riesgo grave para éste, tales como, el origen étnico, el estado de salud presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

De los anteriores, se identificó que se trabaja sobre todo con dos categorías: Datos de Identificación y datos sensibles, ya que como datos patrimoniales se recaban Numero de cuentas bancarias, estados de cuenta, CLABE interbancaria, institución bancaria, facturas, beneficiarios, datos contenidos en declaraciones patrimoniales, y Descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil).

En un segundo momento, para la determinación del riesgo sobre esa tipología de datos personales se valoró la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación (ciclo de vida), en correspondencia con la cantidad de datos involucrados, se materialice uno o más factores que pueden causar un daño a su titular (amenaza).

Para el desarrollo del análisis, se recuperaron cuatro tipos de amenazas sustentados en la Ley:

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizado.
- Pérdida o destrucción no autorizada.

A partir de lo anterior, se consideró una probabilidad baja, media o alta de que la amenaza suceda en las distintas etapas de vida y tipo de datos personales.Además, se tomó en cuenta la consecuencia desfavorable que podría sufrir el titularen caso de vulneración, la cual puede ser leve, moderada o grave.

En cuanto a la valoración del riesgo por el tipo de dato en cada proceso en el que las unidades administrativas del Instituto tratan datos personales, se señaló una escala del 0 al 2, representándose de la forma siguiente:

TIPO DE DATO	RIESGO INHERENTE	NIVEL DE RIESGO
Datos identificativos	Bajo	1
Datos laborales, de domicilio laborales, patrimoniales, procedimientos administrativos	Medio	2
Datos de tránsito y movimientos migratorios; de salud, biométricos	Medio	3
Datos sensibles	Alto	4

Como resultado del levantamiento de información para el análisis de riesgo y de brecha, se identifica que en el Instituto se cuenta con 7 unidades administrativas en las que tienen lugar tratamientos de datos personales para el desarrollo de los 26 procesos como se ilustra a continuación:

Dirección de Admnistración y Finanzas
- **8 tratamientos**

Dirección Jurídica
- **7 Tratamientos**

Dirección de Verificación y Tecnologías de la Información
- **4 tratamientos**

Dirección de Capacitación y Promoción de la Transparencia
- **2 tratmientos**

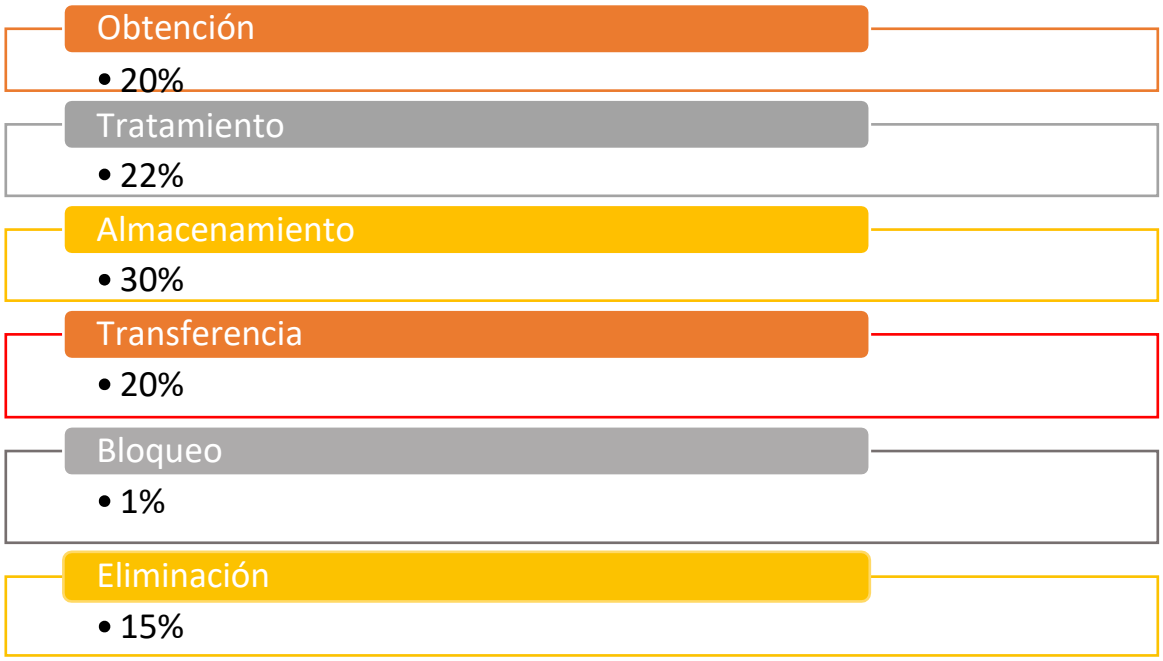
Dirección de Vinculación y COmunicación Social
- **2 tratamientos**

Unidad de Transparencia
- **2 tratamientos**

Área Verificadora de Archivos
- **1 tratamiento**

La unidad administrativa que observa mayor estado de vulnerabilidad y riesgo de los datos personales es la Unidad de Transparencia con 2.38 de riesgo, seguida en orden descendente por la Dirección de Vinculación con 2.25 de riesgo, la dirección de Verificación y Tecnologías de la Información con 2.06 de riesgo, mientras que la Dirección Jurídica y el Área Coordinadora de Archivo tienen un promedio de 2.0 de riesgo; en cuanto en la Dirección de Capacitación y Promoción de Transparencia posee 1.5 de riesgo, concluyendo con la Dirección de Administración y Finanzas con 1.34 de riesgo.

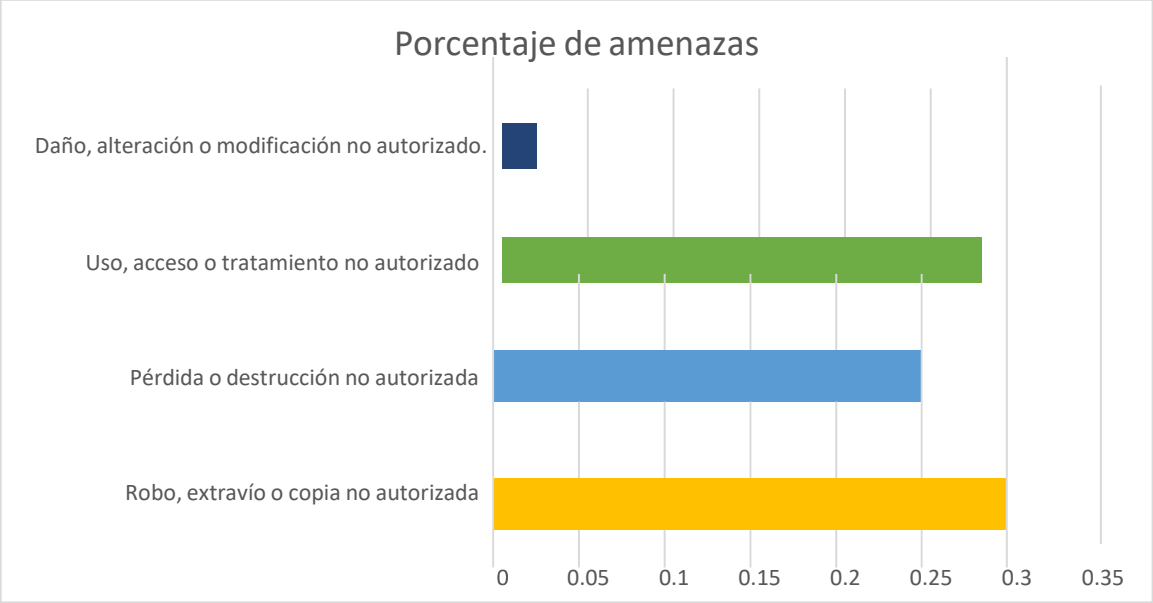
Al respecto, hay que señalar además que la etapa del ciclo de vida (obtención, tratamiento, almacenamiento, transferencia, bloqueo y eliminación) en la que los datos personales se encuentran más vulnerables, es en el periodo de almacenamiento en un 30%; mientras que el periodo que implica menor riesgo es el de bloqueo con un 1%.



Las amenazas a las que se ven expuestos son básicamente:

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizado.
- Pérdida o destrucción no autorizada.

Siendo la más alta, la de robo, extravío o copia no autorizada y la de menor riesgo es daño, alteración o modificación no autorizada, como se muestra en la tabla siguiente:

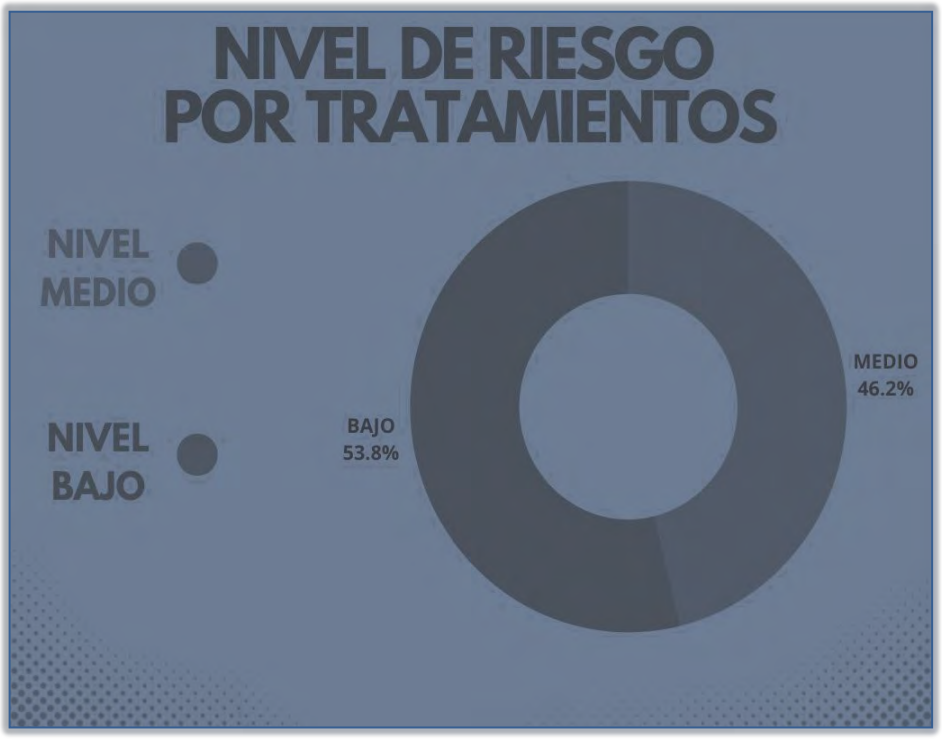


Finalmente, como parte del análisis es posible establecer que el nivel de riesgo es mayormente medio, debido que se trabaja sobre todo con datos de identificación, en algunos casos con datos sensibles y se utilizan en mínimos procesos datos patrimoniales. Asimismo, los datos personales corresponden a menos de 1000 personas, lo que reduce el nivel de riesgo y se mantienen a resguardo en computadoras personales con contraseña y en archiveros ubicados en las unidades administrativas.

El nivel de riesgo por área administrativa se ilustra en la siguiente tabla:

Podemos observar que por las funciones que se desempeñan en las áreasadministrativas, el riesgo no asciende a grave, es así como el nivel medio prevalece con mayor porcentaje, debido a que 5 áreas de las 7 que conforman este Instituto poseen un promedio nivel 2 equivalente a nivel medio, por tratar algunos datos sensibles, patrimoniales e identificativos en sus procesos, conformándose el 28.6%. Solo dos áreasse encuentran en un nivel bajo debido a que los datos que se solicitan para realizar el tratamiento son identificativos.

La siguiente grafica refleja el nivel de riesgo por tratamientos, identificándose 26 procesos con manejo de Datos Personales, los cuales 14 tienen un nivel bajo de riesgo conformando el 53.8%, y 56.2% con nivel medio de riesgo, resultando el 100% de los procesos generados.



8. ANÁLISIS DE BRECHA

Las medidas de seguridad administrativas, físicas y técnicas que actualmente se aplican en el Instituto para mantener la confidencialidad e integralidad de la información, protegiendo los datos personales contra daño, pérdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado e impedir la divulgación no autorizada, son las siguientes:

a) Medidas Administrativas

1. Diseño y desarrollo de un modelo de capacitación permanente en materia de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), impartido a quienes laboran en el Instituto.
2. Diseño y ejecución de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.
3. Aplicación de estrategias de seguridad, para el resguardo de los expedientes, con observancia de criterios vinculados con el sistema de gestión documental.
4. Diseño e implementación de una carta responsiva por parte del personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.
5. Previsión de reportes de incidencias, mediante la elaboración e implementación de los formularios correspondientes.

b) Medidas Físicas

1. Protección de documentos e información resguardándolos en archivos físicos de trámite y concentración, asegurados con llave.
2. Disponer de instalaciones aseguradas con llave para mantener control de acceso de personas a espacios de resguardo de información.
3. Aplicar la firma de cartas de confidencialidad con el personal que trata datos personales

c) Medidas Técnicas

1. Garantizar la seguridad de los datos personales, utilizando claves de usuario y contraseñas de manera individual y evitar compartirlas, prestarlas o registrarlas a la vista de otras personas, y que estas sean seguras al

incluir: caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero.

2. Cuando se identifique algún caso en el que las claves de usuario y/o contraseña hayan sido utilizadas por un tercero, notificar de manera inmediata a la Dirección de Verificación y Tecnologías de la Información, para las prevenciones conducentes.
3. Procurar la utilización de una cuenta de correo electrónico oficial para fines relacionados con las actividades laborales, evitando remitir datos personales.
4. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de restringir el acceso a los datos personales que pudieran mantenerse en archivos y equipos.
5. Cuidar que en los equipos de impresión no se dejen olvidados documentos que contengan datos personales.

9. CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

Los sistemas tecnológicos del Instituto son bastante básicos, por lo que no se aplican controles de identificación y autenticación de usuarios sofisticados. La única medida que se implementa es el uso de contraseñas par el acceso a los equipos de cómputo, repositorios y cuentas de correo institucionales; mismas que son controladas por la Dirección de Verificación y Tecnologías de la Información.

10. LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

El ITAIPCH cuenta con un contrato de servicios con la empresa Digital Server, que provee de repositorios para el almacenaje y respaldo de la información de algunos equipos; sobre todo la que se genera en correos institucionales y la página web institucional; lo que, posibilita los procedimientos de respaldo y recuperación de la información; además, en cada área los respaldos de datos personales se llevan a cabo de acuerdo con las posibilidades identificadas de manera particular. Enalgunos casos se realizan respaldos en la nube de diferentes sistemas operativos, así como en discos duros y otros medios portátiles controlados y administrados por los responsables de cada tratamiento, que permiten el respaldo y la recuperación

de los datos personales cuando así se requiera.

11. EL PLAN DE CONTINGENCIA

Dentro de la seguridad informática se denomina plan de contingencia, a la definición de acciones a realizar, recursos a utilizar y personal a emplear en caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización. Es decir, es la determinación precisa del quién, qué, cómo, cuándo y dónde ocurrió, en caso de producirse una anomalía en el sistema de información.

El plan de contingencia debe considerar todos los componentes del sistema: Datos críticos, equipo lógico de base, aplicaciones, equipos físicos y de comunicaciones, documentación y personal. Además, debe contemplar también todos los recursos auxiliares, sin los cuales el funcionamiento de los sistemas podría verse seriamente comprometido: suministro de potencia; sistemas de climatización; instalaciones; etc.

Debido a que en el ITAIPCH no contamos con sistema tecnológico complejo, tampoco se ha diseñado un plan de contingencia institucional en esos términos, todo se deriva de las medidas de seguridad implementadas de manera específica en cada área. Sin embargo, se cuenta con la posibilidad de recuperar los datos almacenadas en los repositorios y unidades de almacenaje con las que cuenta cada área.

Para contar con un sistema de seguridad mas fortalecido, es necesario contar con el protocolo de actuación en caso de contingencia, que incluya

- Los reportes de vulneración,
- Designación de personas encargadas de
    - Reportar la vulneración,
    - Realizar la investigación para identificar la causa y responsable de la vulneración,
- Método para la notificación de los titulares afectados y
- Procedimientos para la recuperación de la información

12. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES

La destrucción y borrado de información es un tema de vital importancia para proteger la privacidad, confidencialidad, integridad y disponibilidad de la información, y en particular de los datos personales; debe hacerse bajo procedimientos que garanticen que fueron eliminados en su totalidad y que no pueden ser recuperados, y utilizarse de manera indebida.

No obstante, hasta el momento no se han desarrollado en el instituto de manera sistemática y organizada, un sistema de técnicas para la supresión y borrado seguro, todo se hace de acuerdo con la iniciativa y posibilidad de cada área; por lo que este procesoserá parte del plan de trabajo a desarrollar en el futuro inmediato. Por lo anterior, es posible afirmar que será necesaria la implementación de técnicas para la supresión y el borrado seguro que considere tanto métodos físicos que se basan en la destrucción de los medios de almacenamiento físicos electrónicos; como lógicos, basados en la limpieza de los datos almacenados en los equipos de cómputo a través de la desmagnetización y la sobre – escritura.

Lo anterior implica algunas acciones, entre las que podemos contar:

- Capacitación al personal para acercarse al conocimiento de lo que son las técnicas para la supresión y el borrado seguro
- Diseño de un lineamiento para garantizar el proceso
- Adquisición de trituradoras para la destrucción de los documentos
- Implementación de herramientas digitales para
    - la destrucción de medios de almacenamiento electrónicos,
    - la desmagnetización y sobre escritura de los equipos de cómputo

13. PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

Conforme al análisis de brecha, es importante generar acciones que permitan la seguridad de la información, así como de su localización, para resolver de manera

eficaz el acceso, rectificación, corrección u oposición de las personas titulares de la información; por lo que a continuación se presentan las actividades generales que se planea realizar:

- Celebración de reuniones de trabajo con unidades administrativas a efecto identificar alternativas de solución técnicas, físicas y administrativas a desarrollar en el mediano y largo plazo.
- Promover un sistema de gestión y administración de datos personales que permita centralizar mediante la identificación de datos por categorías, asociando los diversos tratamientos y procesos a las políticas de seguridad que resultan aplicables a cada caso, conforme a los estándares y mejores prácticas en la materia.
- Elaborar un protocolo para la protección y el tratamiento de los datos personales.
- Implementar mecanismos de divulgación y conocimiento de las políticas generales de seguridad y, verificar de manera continua su cumplimiento.
- Fortalecer los mecanismos de control de documentos e información en las distintas unidades administrativas, a efecto de evitar posibles vulneraciones.

14. MONITOREO DE LAS MEDIDAS DE SEGURIDAD

Como parte del programa de protección de datos personales, es importante la supervisión de las medidas de seguridad técnicas y físicas, como un elemento para la mejora continua, que permite definir nuevas formas de monitoreo, de acuerdo con las necesidades surgidas al interior del Instituto, como son:

a. Revisión y actualización permanente de las contraseñas utilizadas para resguardar los datos personales en equipos de cómputo.
b. Revisar de manera permanente el cumplimiento de protocolos implementados para la protección de los datos personales.
c. Vigilar que el ingreso de personas sea a través de los accesos correspondientes plenamente identificados.

La Dirección de Capacitación será la encargada de dicho monitoreo, en tanto el Instituto no cuente con una Dirección en materia de Protección de Datos Personales

15. PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

La aplicación del Programa de Protección de Datos Personales en el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales, requiere como un factor esencial, la formación y sensibilización de las personas servidoras públicas, de tal forma que pueda garantizarse la actualización y mejora continua del inventario de datos personales, la observancia de la normatividad, por lo que se propone un programa de capacitación en el tema de protección de datos personales que favorezca la profundización en el conocimiento del tema por parte de quienes intervienen en el tratamiento de datos personales. A manera de propuesta, se han considerado los siguientes temas:

I) La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en Chiapas.
- Antecedentes
- Principios.
- Alcances
- Objetivo
- Implicaciones

II) Obligaciones en la observancia de la LPDPPSOCHIS
- Deberes.
- Medidas de seguridad.
- Procedimientos y sanciones.
- Derechos ARCO (Acceso, Rectificación, Cancelación yOposición).
- Medios de defensa.

III) El programa de protección de datos personales
- Sistemas de datos personales.
- Inventario y Base de Datos.
- Medidas de seguridad.
- Análisis de brecha y riesgo.
- Funciones y obligaciones.

IV) El principio de información: Avisos de Privacidad en el marco del programa de protección de datos personales.
- Contenido: Integral, simplificado
- Consentimiento.
- Deber de información.

- Finalidades del tratamiento de los datos

V) Implementación de medidas de seguridad

- Esquema de privilegios en el acceso
- Registro y control de accesos a las bases de datos
- Identificación y autenticación de usuarios
- Almacenamiento, respaldo y recuperación de la información
- Técnicas para la supresión y borrado seguro de la información

ESTADO DE CHIAPAS

INSTITUTO DE TRANSPARENCIA
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES
CHIAPAS TRANSPARENTE

INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADOS DE CHIAPAS

DIRECCIÓN DE CAPACITACIÓN Y PROMOCION DE LA TRANSPARENCIA

12a Poniente Norte No 1004
Fraccionamiento El Mirador
Tuxtla Gutiérrez, Chiapas. C.P. 29030

Teléfono 961 550 0748

Correo electrónico:
capacitacion@itaipchiapas.org.mx
capacitacioniaipchiapas@gmail.com.mx

www.itaipchiapas.org.mx